Performance Measure Profile

Information Security

FY 2013 Methodology Report

Federal Aviation Administration

Performance Measure Applicability	
☐ **DOT Strategic Plan** Goal: n/a Outcome: n/a Metric: n/a	☒ **Destination 2025** Goal: Move to the Next Level of Safety Outcome: Aviation risk is reduced through all phases of flight (gate-to-gate). Metric: Ensure no cyber security event significantly degrades or disables a mission-critical FAA system.
☐ **Agency Priority Goal**	

FY 2013 Performance Target

Ensure no cyber security event significantly degrades or disables a mission-critical FAA system.

Lead Organization: Finance and Management (AFN)

	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Target	0	0	0	0	0
Actual	0	0	0	0	TBD

Definition of Metric

Metric Unit:	100% of FAA Federal Information System Security Management Act (FISMA) reportable High impact systems shall be recovered in accordance with the Maximum Tolerable Downtime (MTD) identified in their Information Security Contingency Plans (ISCP).
Computation:	The time the system is not available minus the MTD documented in the system ISCP. Time is measured per cyber incident and in hours, as each System's ISCP documents the MTD in hours. Measurement applies to each high impact system individually.
Formula:	The MTD exceeded in each of the FAA high impact systems.
Scope of Metric:	The metric is applicable to the FISMA Reportable HIGH impact systems.
Method of Setting Target:	The target was selected based on an identification of FISMA reportable systems categorized as High impact, a review of the ISCP for each of those systems to determine the MTD, and coordination with the system and business owners in an effort to develop a maturity model for the recovery of these systems and the impact to agency services.

Why the FAA and/or DOT Choose this Metric

Attackers seek to disrupt or exploit critical infrastructure across the United States. One critical infrastructure, as identified by the President in Homeland Security Presidential Directive 7 (HSPD 7), is the nation's transportation infrastructure, including aviation. Accordingly, the FAA, whose mission is to ensure the safe and efficient movement of aircraft, must protect critical infrastructures against the threat of cyber-attack. AIO has the agency lead for ensuring these attacks do not significantly degrade FAA mission-critical systems.

In FIPS 199, confidentiality, integrity, and availability are defined as *security objectives* for information and

information systems:

- **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** "Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system**:**

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

Result in major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Public Benefit

The public benefits from an efficient, safe and secure National Airspace with no disruption of service.

Partners

The external partners working with the agency to achieve this goal are commercial off-the-shelf (COTS) software and hardware vendors. These partners, with their development and support staff, keep operating system software used in the agency up-to-date and secure. In addition, agency internal Line of Business (LOB) partners administer and maintain the specific systems that are identified as High. The LOB system owners will monitor these systems and report when an outage has caused the system to exceed its identified MTD. The AFN organization and internal LOB partners will work together to determine the cause and extent of the disruption to FAA services.

External Factors Affecting Performance

External factors include:

- Natural Disasters or severe weather events
- Hacker's or Nation State actors seeking to exploit system vulnerabilities to disrupt systems service.

Source of the Data

Data on the FISMA reportable high systems is managed and maintained by LOB information technology operators and system owners. FAA's FY 2013 Federal Information Processing Standard (FIPS 199 *High* Impact Systems as defined in the current system Authorization include:

- 110A Inspector Credentials;
- Aviation Safety Hotline Information System;
- Aviation Safety Knowledge Management Environment Enterprise Services;
- Air Transportation Oversight System;
- Office of Aviation Safety External Safety and Mobility Services;
- Office of Aviation Safety Infrastructure;
- Registry Systems;
- AVS Service Oriented Architecture-Infrastructure;
- Electrocardiogram Subsystem;
- Enhanced Flight Standards Automation System;
- Enforcement Information System;
- Enforcement Information System Query and Browse;
- Flight Standards Information Management System;
- Integrated Airman Certification and Rating Application;

- Integrated Rulemaking Management Information System;
- Medical Support Systems;
- Regulatory Guidance Library;
- Safety Performance Analysis System;
- Toxicology Database;
- Whistleblower Protection Program;
- Web Operations Safety System

Statistical Issues

The determination of performance target is achieved by collaboration between the LOB system owner, AFN security and the business partnership management team members.

Completeness

The system owners work collaboratively to determine if there is a disruption to one or more of their high impact systems. They use ISCP MTD data to validate the target. A disruption is defined as when a confirmed cyber event negatively impacted availability, ie, the documented MTD for a system was exceeded.

Reliability

The ISCP captures the MTD for systems based on the Business Impact Analysis (BIA). These systems are continually monitored and assessed.